$\Gamma_{\mathbb{G}}$-базисы: ещё один взгляд на полиномиальные системы

Марк Г. Краузе (**eisgebirgemann@ya.ru**)

Механико-математический факультет, МГУ им. Ломоносова

Предисловие

В последнее время весьма бурно развивается направление коммутативной алгебры, связанное с изучением полиномиальных систем и идеалов. В многом такое развитие обусловлено скачком в развитии теории базисов Грёбнера[1], которые являются в этой области одним из основных инструментов. И хотя «стандартный базис» является важным и неотъемлемым объектом этой теории, у него есть недостатки, вытекающие из достоинств. Одним из таких недостатков является некоторая «ограниченность переносимых свойств», т.е. за большую универсальность и функциональность мы платим потерей части свойств того или иного идеала применительно к стандартному базису. Например, если образующие идеала инвариантны относительно перестановок переменных, то для элементов базиса Грёбнера это не обязательно так, и в этом легко убедиться даже на простых примерах, взять хотя бы идеал $(x + y, xy)$. Возникает вопрос: а можно ли, пожертвовав немного универсальностью и функциональностью, придумать (хотя бы для каких-то классов идеалов) такой базис, который бы сохранял нужные нам свойства. Для того чтобы найти ответ на этот вопрос, нам, возможно, придётся отказаться даже от концепции «мономиального упорядочения» (которая, как известно, является краеугольным камнем теории базисов Грёбнера) и использовать что-то другое. В данной статье делается обзор теории $\Gamma_{\mathbb{G}}$-базисов (в частности, базисов Маколея[2]), которые в какой-то степени решают поставленную задачу, и некоторые современные их приложения. Мы предполагаем, что читатель знаком с основными результатами теории базисов Грёбнера, все они будут использованы нами без доказательств, тем более, что их можно найти во многих книгах, посвящённых теории идеалов (см. [1]). В описании приложений используюся элементы теории численных методов и полиномиальной интерполяции. Все вычисления в примерах были проделаны с использованием системы компьютерной алгебры JAS (http://krum.rz.uni-mannheim.de/jas/).

1. Основные определения

С этого момента и на протяжении всей статьи $\mathfrak{P}$ обозначает алгебру полиномов $\mathbb{K}[x_1, \ldots, x_n]$ над полем $\mathbb{K}$ (там, где это необходимо, мы используем конкретные поля, например, поле комплексных чисел $\mathbb{C}$, но это оговаривается отдельно). Через (S) будем обозначать идеал кольца $\mathfrak{P}$, порождённый семейством полиномов $S \subseteq \mathfrak{P}$.

Теорема 1.1 (Теорема Гильберта[3] о базисе) Всякий идеал кольца $\mathfrak{P}$ порождается конечным семейством полиномов этого кольца.

Доказательство: [1], гл. 2, §5. □

[1] Wolfgang Gröbner (1899 - 1980) — австрийский математик, его имя невольно возникает в связи с базисами Грёбнера, открытыми его учеником Бруно Бухбергером (Bruno Buchberger) и названными им в честь своего учителя.

[2] Francis Sowerby Macaulay (1862 - 1937) — английский математик, который внёс большой вклад в развитие алгебраической геометрии.

[3] David Hilbert (1862 - 1943) — выдающийся немецкий математик, внёс огромный вклад в развитие всей математики в целом.

С этого момента, если не сказано обратное, мы полагаем S конечным. Пусть Γ — аддитивный коммутативный моноид, снабжённый линейным порядком $\prec$ таким, что выполнена следующая аксиома:

$$\mathbf{T} : \forall \alpha, \beta, \gamma \in \Gamma \quad (\alpha \prec \beta) \Longrightarrow (\alpha + \gamma \prec \beta + \gamma).$$

В ряде случаев помимо аксиомы $\mathbf{T}$ мы будем требовать выполнения ещё одной аксиомы:

$$\mathbf{P} : \forall \alpha \in \Gamma \quad (0 \preceq \alpha).$$

В этом случае мы для краткости будем говорить, что указанный порядок является *положительным.*

Замечание 1.1 Заметим, что выполнения аксиом $\mathbf{T}$ и $\mathbf{P}$ достаточно для того, чтобы $\prec$ вполне упорядочивал Γ. Это является существенным в теории базисов Грёбнера (в этом случае $\Gamma = \mathbb{Z}^m_{\geqslant 0}$). Для нас особенно важным будет случай, когда $\Gamma = \mathbb{Z}_{\geqslant 0}$.

Определение 1.1 Семейство линейных подпространств $\mathbb{G} = \{\mathscr{P}_\gamma \,|\, \gamma \in \Gamma\}$ алгебры $\mathfrak{P}$ называется *градуировкой* (*индуцируемой* Γ) *на* $\mathfrak{P}$, если

$$\mathfrak{P} = \bigoplus_{\gamma \in \Gamma} \mathscr{P}_\gamma \quad \text{и} \quad \forall \alpha, \beta \in \Gamma \quad (f \in \mathscr{P}_\alpha) \wedge (g \in \mathscr{P}_\beta) \Longrightarrow (f \cdot g \in \mathscr{P}_{\alpha+\beta}).$$

Если задана какая-то градуировка на $\mathfrak{P}$, любой ненулевой полином $f \in \mathfrak{P}$ единственным образом представляется в виде:

$$f = \sum_{i=1}^{n} f_{\gamma_i}, \quad \gamma_1 \prec \ldots \prec \gamma_n, \quad \forall i \in \{1, \ldots, n\} \quad f_{\gamma_i} \in \mathscr{P}_{\gamma_i}, \quad f_{\gamma_i} \neq 0.$$

Определение 1.2 Определённый выше полином f_{γ_n} называется *максимальной частью* (или *старшей* $\Gamma_{\mathbb{G}}$*-компонентой*) полинома f по отношению к градуировке $\mathbb{G}$ (мы будем обозначать её через $\mathbf{mp}(f, \mathbb{G})$ или просто $\mathbf{mp}(f)$, если ясно, о какой градуировке идёт речь). Элемент γ_n называется $\Gamma_{\mathbb{G}}$*-степенью* f (обозн. $\mathbf{d}_{\mathbb{G}}(f)$). Все остальные полиномы f_{γ_i} называются *младшими* $\Gamma_{\mathbb{G}}$*-компонентами* f.

Определение 1.3 Полином $\mathbf{rp}(f) = f - \mathbf{mp}(f)$ называется *остаточной частью* полинома f по отношению к $\mathbb{G}$.

Примеры:
1.1) Одним из важнейших примеров градуировки является так называемая «градуировка по степеням», т.е. когда $\Gamma = \mathbb{Z}_{\geqslant 0}$ (с естественным положительным порядком) и

$$\mathscr{P}_\gamma = \{f \in \mathfrak{P} \,|\, f = 0 \text{ или является однородным полиномом степени } \gamma\}.$$

Такую градуировку мы будем обозначать через $\mathbf{H}$. Мы также будем полагать, что в случае такой градуировки $\mathbf{mp}(0, \mathbf{H}) = 0$ по определению.
1.2) Другим важным примером является знакомая из теории базисов Грёбнера «градуировка по мономам». В этом случае

$$\Gamma = \mathbb{Z}^m_{\geqslant 0}, \quad \mathscr{P}_\gamma = \{c \cdot \prod_{i=1}^{m} x_i^{\gamma_i} \,|\, c \in \mathbb{K}\} \quad \text{для} \quad \gamma = (\gamma_1, \ldots, \gamma_m).$$

Нетрудно видеть, что для всякого $f \in \mathfrak{P}$ выполнено $\mathbf{mp}(f) = \mathbf{lc}(f) \cdot \mathbf{lm}(f)$, где $\mathbf{lm}(f)$ — старший моном f (в смысле допустимого мономиального упорядочения $\prec$), а $\mathbf{lc}(f)$ — коэффициент, с которым он входит в f. Такую градуировку мы будем обозначать через $\mathbf{G}$.

Определение 1.4 Множество $\mathscr{H} = \{h_1, \ldots, h_n\} \subseteq \mathfrak{P} \backslash \{0\}$ называется $\Gamma_{\mathbb{G}}$-*базисом* идеала I кольца $\mathfrak{P}$, если $I = (h_1, \ldots, h_n)$ и для любого ненулевого $f \in I$ существуют такие $q_1, \ldots, q_n \in \mathfrak{P}$, что

$$f = \sum_{i=1}^{n} q_i h_i \quad \text{и} \quad \forall i \in \{1, \ldots, n\} \quad \mathbf{d}_{\mathbb{G}}(q_i) + \mathbf{d}_{\mathbb{G}}(h_i) \leqslant \mathbf{d}_{\mathbb{G}}(f).$$

Такое представление полинома f называется $\Gamma_{\mathbb{G}}$-*представлением* f относительно $\mathscr{H}$.

Определение 1.5 Пусть $f \in \mathfrak{P}$, $S = \{f_1, \ldots, f_m\}$. Будем говорить, что f *редуцируется к* $\widetilde{f}$ *относительно* S *за один шаг*, если $\mathbf{d}_{\mathbb{G}}(\widetilde{f}) < \mathbf{d}_{\mathbb{G}}(f)$ и

$$\exists\, q_1, \ldots, q_m \in \mathfrak{P}: \quad \widetilde{f} = f - \sum_{i=1}^{m} q_i f_i, \quad \forall i \in \{1, \ldots, m\} \quad \mathbf{d}_{\mathbb{G}}(q_i) + \mathbf{d}_{\mathbb{G}}(f_i) \leqslant \mathbf{d}_{\mathbb{G}}(f).$$

Будем говорить, что f *редуцируется к* $\widetilde{f}$ *относительно* S *за* k *шагов*, если f каким-то образом редуцируется к $\widetilde{f}$ последовательным применением k одношаговых редукций.

$$\text{Обозначение}: \quad f \rightarrowtail \widetilde{f} \pmod{S, k}.$$

Определение 1.6 Пусть $f \in \mathfrak{P}$, $S = \{f_1, \ldots, f_m\}$. Будем говорить, что f *редуцируется к* $\widetilde{f}$ *относительно* S, если существует такое $k \in \mathbb{N}$, что $f \rightarrowtail \widetilde{f} \pmod{S, k}$.

$$\text{Обозначение}: \quad f \rightarrowtail \widetilde{f} \pmod{S, *}.$$

Лемма 1.1 Пусть $S = \{f_1, \ldots, f_n\}$, $I = (S)$. Следующие условия эквивалентны:
a) S — $\Gamma_{\mathbb{G}}$-базис I,
b) $(\mathbf{mp}(f_1), \ldots, \mathbf{mp}(f_n)) = (\{\mathbf{mp}(f) \,|\, f \in I\})$,
c) $\forall f \in I \quad f \rightarrowtail 0 \pmod{S, *}$.

Доказательство: a) $\Longrightarrow$ b). Пусть $f \in \mathfrak{P}$, $f = \sum_{i=1}^{n} q_i f_i$ — какое-то его $\Gamma_{\mathbb{G}}$-представление, $X = \{j \,|\, \mathbf{d}_{\mathbb{G}}(q_j f_j) = \mathbf{d}_{\mathbb{G}}(f)\}$. Тогда

$$\mathbf{mp}(f) = \sum_{j \in X} \mathbf{mp}(q_i)\mathbf{mp}(f_i),$$

откуда и следует b).
b) $\Longrightarrow$ c). Если $f = 0$, доказывать нечего. Пусть теперь $f \in I \backslash \{0\}$. По предположению существуют такие $q_1, \ldots, q_n \in \mathfrak{P}$, что $\mathbf{mp}(f) = \sum_{i=1}^{n} q_i \mathbf{mp}(f_i)$. Рассмотрим определённое выше множество X. Тогда $\mathbf{mp}(f) = \sum_{j \in X} \mathbf{mp}(q_j)\mathbf{mp}(f_j)$. Применив одношаговую редукцию:

$$f \rightarrowtail \widetilde{f} \stackrel{\text{def}}{=} f - \sum_{j \in X} \mathbf{mp}(q_j) f_j \pmod{S, 1},$$

можно прийти к полиному $\widetilde{f}$, который имеет меньшую (чем f) степень, но при этом остаётся в идеале. Продолжая этот процесс, в конце концов получим, что вновь отредуцированный

полином или равен 0, или имеет степень 0, т.е. принадлежит $\mathbb{K}\backslash\{0\}$, что также легко редуцируется к 0 (ибо в этом случае $I = (1)$), откуда ясно, что $f \rightarrowtail 0 \pmod{S, *}$.
c) $\Longrightarrow$ a). Пусть $f \in I$, $f \rightarrowtail 0 \pmod{S, k}$, т.е.

$$\exists\, g_0 \ldots, g_k : \quad f = g_0 \rightarrowtail g_1 \rightarrowtail \ldots \rightarrowtail g_k = 0 \pmod{S, 1},$$

и $\mathbf{mp}(g_{j-1}) = \sum \mathbf{mp}(q_{ji})\mathbf{mp}(f_i)$, $j = 1, \ldots, k$, в смысле указанных выше обозначений. Тогда

$$f = \sum_{i=1}^{n} \sum_{j=1}^{k} \mathbf{mp}(q_{ji}) f_i$$

является $\Gamma_{\mathbb{G}}$-представлением f, откуда ясно, что S — $\Gamma_{\mathbb{G}}$-базис I. □

Определение 1.7 Идеал I кольца $\mathfrak{P}$ называется $\Gamma_{\mathbb{G}}$-*однородным*, если для любого $f \in I$ каждая $\Gamma_{\mathbb{G}}$-компонента полинома f принадлежит I.

Лемма 1.2 (Лемма Кёнига[4]) Идеал I кольца $\mathfrak{P}$ является $\Gamma_{\mathbb{G}}$-однородным тогда и только тогда, когда $I = (f_1, \ldots, f_m)$, где $f_1, \ldots, f_m$ — $\Gamma_{\mathbb{G}}$-компоненты.

Доказательство: Аналогично доказательству из [1], гл. 8, §3. □

Теорема 1.2 Всякий идеал I кольца $\mathfrak{P}$ обладает $\Gamma_{\mathbb{G}}$-базисом.

Доказательство: Поскольку всякий идеал кольца $\mathfrak{P}$ обладает конечным базисом, в силу леммы 1.1 вопрос существования $\Gamma_{\mathbb{G}}$-базиса идеала I можно свести к вопросу существования у идеала $(\{\mathbf{mp}(f) \mid f \in I\})$ конечного базиса, состоящего из $\Gamma_{\mathbb{G}}$-компонент. Но по лемме Кёнига такой базис всегда существует, следовательно, идеал I обладает $\Gamma_{\mathbb{G}}$-базисом. □

Если проводить аналогии с теорией базисов Грёбнера, читателю могут показаться знакомыми формулировки пунктов из леммы 1.1. Тем не менее, это существенно расширяет круг рассматриваемых базисов. Нетрудно проверить, что имеет место следующее утверждение.

Утверждение 1.1 Любой базис Грёбнера идеала I относительно порядкового мономиального упорядочения (т.е. допустимого мономиального упорядочения $\prec$, для которого выполнено следующее свойство: $\forall \alpha, \beta \in \mathbb{Z}^m_{\geqslant 0}$ $(\sum \alpha_i < \sum \beta_i) \Longrightarrow (\alpha \prec \beta)$) является $\Gamma_{\mathbf{H}}$-базисом.

Обратное, вообще говоря, неверно, как показывает следующий пример.

Примеры:
1.3) Пусть $h_1 = x^3y - xy^3$, $h_2 = x^4 + 2x^2y^2 + y^4 - 1$ ($\mathfrak{P} = \mathbb{R}[x, y]$). В этом случае будем иметь:

$$(\{\mathbf{mp}(f, \mathbf{H}) \mid f \in (h_1, h_2)\}) = (x^3y - xy^3, x^4 + 2x^2y^2 + y^4) = (\mathbf{mp}(h_1, \mathbf{H}), \mathbf{mp}(h_2, \mathbf{H})),$$

при этом редуцированный базис Грёбнера идеала (h_1, h_2) (отн. $grlex$-упорядочения) есть

$$\{g_1, \ldots, g_5\} = \{x^3y - xy^3, x^4 + 2x^2y^2 + y^4 - 1, 3x^2y^3 + y^5 - y, 4xy^5 - xy, 4y^7 - 3x^2y - 4y^3\},$$

а редуцированный базис Грёбнера идеала $(x^3y - xy^3, x^4 + 2x^2y^2 + y^4)$ есть

$$\{\widetilde{g}_1, \ldots, \widetilde{g}_5\} = \{x^3y - xy^3, x^4 + 2x^2y^2 + y^4, 3x^2y^3 + y^5, xy^5, y^7\}.$$

[4] Johann Samuel König (1712 - 1757) — немецкий математик.

Таким образом, в силу леммы 1.1 $\{h_1, h_2\}$ и $\{g_1, \ldots, g_5\}$ являются $\Gamma_{\mathbf{H}}$-базисами идеала (h_1, h_2), но при этом $\{h_1, h_2\}$ не является базисом Грёбнера этого идеала.

Немного модифицировав этот пример, можно показать, что не всякий базис Грёбнера идеала I (т.е. базис Грёбнера относительно произвольного допустимого мономиального упорядочения) является $\Gamma_{\mathbf{H}}$-базисом этого идеала.

Примеры:
1.4) Действительно, для того же самого идеала (h_1, h_2) редуцированный базис Грёбнера отн. lex-упорядочения имеет вид:

$$\{g_1, \ldots, g_4\} = \{4y^9 - 5y^5 + y, 4xy^5 - xy, 3x^2y + 4y^7 - 4y^3, 3x^4 - 8y^8 + 11y^4 - 3\},$$

при этом редуцированный базис Грёбнера (отн. lex) идеала $(x^3y - xy^3, x^4 + 2x^2y^2 + y^4)$ есть

$$\{\widetilde{g}_1, \ldots, \widetilde{g}_5\} = \{y^7, xy^5, 3x^2y^3 + y^5, x^3y - xy^3, x^4 + 2x^2y^2 + y^4\}.$$

Поскольку

$$(\mathbf{mp}(g_1, \mathbf{H}), \ldots, \mathbf{mp}(g_4, \mathbf{H})) = (y^7, xy^5) = (\widetilde{g}_1, \widetilde{g}_2) \neq (\widetilde{g}_1, \ldots, \widetilde{g}_5),$$

в силу леммы 1.1 базис Грёбнера $\{g_1, \ldots, g_4\}$ не является $\Gamma_{\mathbf{H}}$-базисом идеала (h_1, h_2).

2. Алгоритм $\Gamma_{\mathbb{G}}$-редукции

В предыдущем разделе мы ввели понятие $\Gamma_{\mathbb{G}}$-базиса, показали на примере градуировки $\mathbf{H}$ его связь с базисом Грёбнера, доказали, что всякий идеал $I \lhd \mathfrak{P}$ обладает $\Gamma_{\mathbb{G}}$-базисом, но при этом не предъявили никакого способа его вычисления. В этом разделе речь пойдёт об алгоритме $\Gamma_{\mathbb{G}}$-редукции, который в каком-то смысле обобщает стандартную редукцию в алгоритме Бухбергера (см. [1]), а в следующем разделе мы поговорим о способах построения $\Gamma_{\mathbb{G}}$-базиса. С этого момента, если не оговорено отдельно, мы считаем, что во всех рассуждениях используется какая-то заранее фиксированная градуировка $\mathbb{G}$. Через $\mathfrak{P}_d \subseteq \mathfrak{P}$ обозначим линейное пространство полиномов, $\Gamma_{\mathbb{G}}$-степень которых не превосходит d, а через $\mathfrak{P}_d^{\mathfrak{H}}$ — линейное пространство $\Gamma_{\mathbb{G}}$-компонент, $\Gamma_{\mathbb{G}}$-степень которых равна d. Мы также введём сокращение $f^{\mathfrak{H}}$, обозначающее $\mathbf{mp}(f, \mathbb{G})$, в дальнейшем будем обозначать идеал $(\{f^{\mathfrak{H}} \,|\, f \in I\})$ через $I^{\mathfrak{H}}$ (сразу отметим, что здесь замкнутость относительно сложения требуется только для полиномов из одного $\mathscr{P}_\gamma$), а соответствующее множество $\{h^{\mathfrak{H}} \,|\, h \in \mathscr{H}\}$ — через $\mathscr{H}^{\mathfrak{H}}$. Сформулируем теперь один из результатов леммы 1.2 в несколько ином виде.

Утверждение 2.1 Множество $\mathscr{H} \subseteq \mathfrak{P}$ является $\Gamma_{\mathbb{G}}$-базисом идеала I тогда и только тогда, когда $(\mathscr{H}^{\mathfrak{H}}) = I^{\mathfrak{H}}$.

Пусть теперь $\Omega = \{p_1, \ldots, p_m\} \subseteq \mathfrak{P}$, $d \in \Gamma$. Для каждой пары (Ω, d) определим линейное пространство

$$V_d(\Omega) \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^{m} q_i p_i^{\mathfrak{H}} \,\middle|\, q_i \in \mathfrak{P}^{\mathfrak{H}}_{d - \mathbf{d}_{\mathbb{G}}(p_i)}, i \in \{1, \ldots, m\} \right\},$$

которое является подпространством пространства $\mathfrak{P}_d^{\mathfrak{H}}$ (в том случае, когда $\mathbf{d}_{\mathbb{G}}(p_i) > d$, мы полагаем $q_i = 0$), и пусть также $\Omega_i = \{p_1, \ldots, p_i\}$, $i = 1, \ldots, m$. Предположим, что на $\mathfrak{P}$ задано какое-то скалярное произведение (о том, какое именно для нас является наиболее удобным, мы поговорим в следующих разделах). Оно индуцирует понятие ортогональности

полиномов, и для каждого подпространства $V_d(\Omega_{i-1})$ мы можем рассмотреть его ортогональное дополнение до всего пространства $V_d(\Omega_i)$. Таким образом, корректно определены следующие пространства:

$$W_d(\Omega_i) \stackrel{\text{def}}{=} V_d(\Omega_{i-1})^{\perp} \subseteq V_d(\Omega_i) \text{ для всех } i = 2, \dots m.$$

Мы также полагаем $W_d(\Omega_1) \stackrel{\text{def}}{=} V_d(\Omega_1)$. В этом случае мы можем представить $V_d(\Omega)$ в виде прямой суммы:

$$V_d(\Omega) = \bigoplus_{i=1}^{m} W_d(\Omega_i),$$

которая, вообще говоря, зависит от порядка полиномов в наборе Ω. Более того, эта сумма может быть избыточной в том смысле, что некоторые $W_d(\Omega_i)$ могут оказаться нулевыми. Это происходит тогда и только тогда, когда для любого $q_i \in \mathfrak{P}^{\mathfrak{H}}_{d-\mathbf{d}_{\mathbb{G}}(p_i)}$ существуют такие $q_k \in \mathfrak{P}^{\mathfrak{H}}_{d-\mathbf{d}_{\mathbb{G}}(p_k)}$, $k = 1, \dots, i-1$, что

$$q_i p_i^{\mathfrak{H}} = \sum_{k=1}^{i-1} q_k p_k^{\mathfrak{H}},$$

что эквивалентно тому, что

$$p_i^{\mathfrak{H}} \cdot \mathfrak{P}^{\mathfrak{H}}_{d-\mathbf{d}_{\mathbb{G}}(p_i)} \subseteq (\Omega^{\mathfrak{H}}).$$

На этом наблюдении основан представленный ниже алгоритм $\Gamma_{\mathbb{G}}$-редукции, который является «надстройкой» над процессом ортогонализации Грама-Шмидта.

Алгоритм 2.1 **($\Gamma_{\mathbb{G}}$-редукция)**

```
# GammaReduction, p ∈ 𝔓.
def GammaReduction(p,Ω):
.    f = p
.    for d in [d_G(p) .. 0]:
.    .    for i in [1 .. m]:
.    .    .    q_id = ComputeQid(f,Ω,i,d)
# Вычисляет полином
```

$$q_{id} = \sum_{k=1}^{i} q_{idk} p_k^{\mathfrak{H}} \in W_d(\Omega_i)$$

```
# такой, что ∀k ∈ {1,...,i} q_idk ∈ 𝔓^𝔥_{d-d_G(p_k)} и f^𝔥 − q_id ⊥ W_d(Ω_i).
.    .    r_d = f^𝔥 - Σ_{i=1}^m q_id
.    .    f = f - r_d - Σ_{i=1}^m Σ_{k=1}^i q_idk p_k
.    return Representation
# Representation: p = Σ_{k=1}^m q_k p_k + r, где
```

$$q_k = \sum_{d=0}^{\mathbf{d}_{\mathbb{G}}(p)} \sum_{i=k}^{m} q_{idk}\,, \quad r = \sum_{d=0}^{\mathbf{d}_{\mathbb{G}}(p)} r_d\,.$$

```
# end-of-GammaReduction
```

Определение 2.1 Полином $f \in \mathfrak{P}$ называется *редуцированным относительно* Ω, если

$$f = \sum_{d=0}^{\mathbf{d}_{\mathbb{G}}(f)} f_d, \ \ f_d \in \mathfrak{P}_d^{\mathfrak{H}}, \ \ f_d \perp V_d(\Omega).$$

Замечание 2.1 Поскольку пространство $V_d(\Omega)$ не зависит от порядка полиномов в Ω, тот факт, что полином является редуцированным относительно Ω, не зависит от этого порядка, но при этом, конечно, зависит от выбора скалярного произведения на $\mathfrak{P}$.

Утверждение 2.2 Полиномы r_d, $d = 0, \ldots, \mathbf{d}_{\mathbb{G}}(p)$, q_k, $k = 1, \ldots, m$, полученные в алгоритме 2.1, обладают следующими свойствами:

$$\mathbf{d}_{\mathbb{G}}(q_k) + \mathbf{d}_{\mathbb{G}}(p_k) \leqslant \mathbf{d}_{\mathbb{G}}(p) \ \text{ и } \ r_d \perp V_d(\Omega).$$

В частности, полином r, полученный в алгоритме $\Gamma_{\mathbb{G}}$-редукции, является редуцированным относительно Ω.

Доказательство: Первое свойство непосредственно вытекает из построения q_k. Проверим выполнение второго свойства индукцией по $s = 1, \ldots, m$, на каждом шагу убеждаясь, что имеет место следующее свойство:

$$f^{\mathfrak{H}} - \sum_{i=1}^{s} q_{id} \perp V_d(\Omega_s).$$

Здесь под f понимается полином, полученный на соответствующем шаге алгоритма 2.1. При $s = m$ это свойство можно переписать в виде:

$$r_d \overset{\text{def}}{=} f^{\mathfrak{H}} - \sum_{i=1}^{m} q_{id} \perp V_d(\Omega),$$

именно его нам и нужно доказать. Для $s = 1$ будем иметь:

$$f^{\mathfrak{H}} - q_{1d} \perp W_d(\Omega_1) \overset{\text{def}}{=} V_d(\Omega_1),$$

что следует из построения q_{1d}. Для осуществления перехода $s - 1 \to s$ вспомним, что по построению

$$q_{sd} \in W_d(\Omega_s) \overset{\text{def}}{=} V_d(\Omega_{s-1})^{\perp} \subseteq V_d(\Omega_s).$$

Учитывая предположение индукции, отсюда следует, что

$$f^{\mathfrak{H}} - \sum_{i=1}^{s} q_{id} = \left(f^{\mathfrak{H}} - \sum_{i=1}^{s-1} q_{id} \right) - q_{sd} \perp V_d(\Omega_{s-1}).$$

Из алгоритма 2.1 также следует, что

$$f^{\mathfrak{H}} - q_{sd} \perp W_d(\Omega_s).$$

Учитывая, что

$$\sum_{i=1}^{s-1} q_{id} \in V_d(\Omega_{s-1}) = W_d(\Omega_s)^{\perp} \subseteq V_d(\Omega_s),$$

получаем нужное соотношение, что и доказывает утверждение. $\square$

Утверждение 2.2 позволяет интерпретировать разложение, полученное в результате алгоритма $\Gamma_{\mathbb{G}}$-редукции, как представление полинома в виде «основной части», которая лежит в идеале (Ω), и редуцированного «остатка» r. В связи с этим введём ещё одно определение, связанное алгоритмом 2.1, оно будет играть очень важную роль в дальнейшем.

Определение 2.2 Полином r, полученный в результате $\Gamma_{\mathbb{G}}$-редукции полинома p относительно Ω, называется $\Gamma_{\mathbb{G}}$-*остатком* полинома p относительно Ω (обозн. $\mathbf{grem}(p,\Omega)$).

Замечание 2.2 Вообще говоря, если полином $\mathbf{grem}(p,\Omega) \neq 0$, он может зависеть от порядка полиномов в Ω. Поэтому в дальнейшем мы предполагаем, что этот порядок заранее фиксирован, хотя очень скоро мы покажем, что в «интересных» нам случаях $\Gamma_{\mathbb{G}}$-остаток не зависит от порядка полиномов в Ω, что делает такую договорённость несущественной.

3. Построение $\Gamma_{\mathbb{G}}$-базиса

В этом разделе мы поговорим о том, как в принципе можно вычислить $\Gamma_{\mathbb{G}}$-базис. И мы начнём с доказательства теорем, на которых основан алгоритм построения.

Теорема 3.1 Пусть $\mathscr{H} = \{h_1, \dots, h_m\}$ — $\Gamma_{\mathbb{G}}$-базис идеала $I = (\mathscr{H})$. Пусть $f \in \mathfrak{P}$ представляется в виде:

$$f = \sum_{i=1}^{m} q_i h_i + r, \quad q_i \in \mathfrak{P}, \; p_i \in \mathscr{H},$$

где $r \in \mathfrak{P}$ — какой-то редуцированный полином. Тогда $r = \mathbf{grem}(f, \mathscr{H})$.

Доказательство: Пусть $\widetilde{q}_i$ и $\widetilde{r}$ — соответственно коэффициенты и $\Gamma_{\mathbb{G}}$-остаток, полученные в результате алгоритма $\Gamma_{\mathbb{G}}$-редукции, применённого к входным данным f, $\mathscr{H}$. Тогда по построению

$$f = \sum_{i=1}^{m} q_i h_i + r = \sum_{i=1}^{m} \widetilde{q}_i h_i + \widetilde{r},$$

откуда следует, что

$$g \stackrel{\text{def}}{=} r - \widetilde{r} = \sum_{i=1}^{m} (\widetilde{q}_i - q_i) h_i \in I.$$

Если $g = 0$, то доказывать нечего. Предположим, что $g \neq 0$. Поскольку полиномы r и $\widetilde{r}$ редуцированы,

$$r^{\mathfrak{H}} \perp V_{\mathbf{d}_{\mathbb{G}}(r)}(\mathscr{H}) \;\text{ и }\; \widetilde{r}^{\mathfrak{H}} \perp V_{\mathbf{d}_{\mathbb{G}}(\widetilde{r})}(\mathscr{H}).$$

Докажем, что $g^{\mathfrak{H}} \perp V_{\mathbf{d}_{\mathbb{G}}(g)}(\mathscr{H})$. В том случае, когда $\mathbf{d}_{\mathbb{G}}(r) \neq \mathbf{d}_{\mathbb{G}}(\widetilde{r})$ (или $\mathbf{d}_{\mathbb{G}}(r) = \mathbf{d}_{\mathbb{G}}(\widetilde{r})$, но при этом $r^{\mathfrak{H}} \neq \widetilde{r}^{\mathfrak{H}}$), это сразу следует из определения полинома g. Осталось рассмотреть случай, когда $\mathbf{d}_{\mathbb{G}}(r) = \mathbf{d}_{\mathbb{G}}(\widetilde{r})$ и $r^{\mathfrak{H}} = \widetilde{r}^{\mathfrak{H}}$. Перепишем g в следующем виде:

$$g = r - \widetilde{r} = (r - r^{\mathfrak{H}}) - (\widetilde{r} - \widetilde{r}^{\mathfrak{H}}),$$

и будем продолжать этот процесс, пока не придём к одному из ранее описанных случаев (в конце концов это произойдёт, т.к. $\Gamma_{\mathbb{G}}$-степени полиномов r и $\widetilde{r}$ после такой замены каждый раз уменьшаются). Следовательно,

$$g^{\mathfrak{H}} \perp V_{\mathbf{d}_{\mathbb{G}}(g)}(\mathscr{H}).$$

Поскольку $\mathscr{H}$ — $\Gamma_{\mathbb{G}}$-базис и $g \in I$, получаем, что $g^{\mathfrak{H}} \in (\mathscr{H}^{\mathfrak{H}})$ и $g^{\mathfrak{H}} \in \mathfrak{P}^{\mathfrak{H}}_{\mathbf{d}_{\mathbb{G}}(g)}$, откуда следует, что

$$g^{\mathfrak{H}} \in (\mathscr{H}^{\mathfrak{H}}) \cap \mathfrak{P}^{\mathfrak{H}}_{\mathbf{d}_{\mathbb{G}}(g)} = V_{\mathbf{d}_{\mathbb{G}}(g)}(\mathscr{H}),$$

это противоречит полученному выше соотношению. Значит, $g = 0$, и теорема доказана. □

Следствие 3.1 Полином $r = \mathbf{grem}(f, \mathscr{H})$, где $\mathscr{H}$ — $\Gamma_{\mathbb{G}}$-базис, не зависит от порядка полиномов в $\mathscr{H}$.

Теорема 3.2 Конечное множество полиномов $\mathscr{H}$ является $\Gamma_{\mathbb{G}}$-базисом идеала $I = (\mathscr{H})$ тогда и только тогда, когда $\mathbf{grem}(f, \mathscr{H}) = 0$ для любого $f \in I$.

Доказательство: Если $\mathscr{H}$ — $\Gamma_{\mathbb{G}}$-базис, то по теореме 3.1 $\mathbf{grem}(f, \mathscr{H}) = 0$, поскольку сам $f \in I$. Необходимость доказана. Для доказательства достаточности рассмотрим какое-нибудь представление

$$f = \sum_{h \in \mathscr{H}} q_h h \in I.$$

Предположим, что

$$\mathbf{d}_{\mathbb{G}}(f) < \max_{h \in \mathscr{H}}\{\mathbf{d}_{\mathbb{G}}(q_h h)\} = \max_{h \in \mathscr{H}}\{\mathbf{d}_{\mathbb{G}}(q_h) + \mathbf{d}_{\mathbb{G}}(h)\}.$$

Тогда существует такое $X \subseteq \mathscr{H}$, что

$$\sum_{h \in X} q_h^{\mathfrak{H}} h^{\mathfrak{H}} = 0.$$

По предположению

$$\mathbf{grem}\left(\sum_{h \in X} q_h^{\mathfrak{H}} h, \mathscr{H}\right) = 0,$$

откуда следует, что

$$\sum_{h \in X} q_h^{\mathfrak{H}} h = \sum_{h \in X} \sigma_h h$$

для некоторых полиномов $\sigma_h \in \mathfrak{P}$, $h \in X$, таких, что

$$\max_{h \in X}\{\mathbf{d}_{\mathbb{G}}(\sigma_h) + \mathbf{d}_{\mathbb{G}}(h)\} < \max_{h \in X}\{\mathbf{d}_{\mathbb{G}}(q_h) + \mathbf{d}_{\mathbb{G}}(h)\}.$$

Положим также $\sigma_h \stackrel{\text{def}}{=} q_h^{\mathfrak{H}}$ для $h \in \mathscr{H} \backslash X$. Тогда

$$f = \sum_{h \in \mathscr{H}} \widetilde{q}_h h, \text{ где } \widetilde{q}_h = q_h - q_h^{\mathfrak{H}} + \sigma_h, h \in \mathscr{H}.$$

Заметим, что

$$\mathbf{d}_{\mathbb{G}}(f) \leqslant \max_{h \in \mathscr{H}}\{\mathbf{d}_{\mathbb{G}}(\widetilde{q}_h h)\} < \max_{h \in \mathscr{H}}\{\mathbf{d}_{\mathbb{G}}(q_h h)\}.$$

Это означает, что, продолжая данный процесс, мы с каждым шагом будем уменьшать максимальную $\Gamma_{\mathbb{G}}$-степень в представлении, не изменяя при этом полином f. Тогда в конце концов мы придём к тому, что

$$\mathbf{d}_{\mathbb{G}}(f) = \max_{h \in \mathscr{H}}\{\mathbf{d}_{\mathbb{G}}(q_h h)\}.$$

Отсюда следует, что $f^{\mathfrak{H}} \in (\mathscr{H}^{\mathfrak{H}})$ для любого $f \in I$. Согласно утверждению 2.1 это и означает, что $\mathscr{H}$ — $\Gamma_{\mathbb{G}}$-базис I. □

Полученный выше результат можно переформулировать в терминах модуля сизигий для полиномов из $\mathscr{H}^{\mathfrak{H}}$, который мы обозначим через $S(\mathscr{H}^{\mathfrak{H}})$ (подробнее см. [1], гл. 2, §9). Осталось лишь заметить, что вместо того, чтобы проверять критерий теоремы 3.2 для всех сизигий из $S(\mathscr{H}^{\mathfrak{H}})$, достаточно проверить его только для базиса этого модуля. Это даёт нам ключевое следствие текущего раздела.

Следствие 3.2 Пусть $\mathscr{H}$ — конечное множество полиномов из $\mathfrak{P}$, $\mathscr{B}$ — базис $S(\mathscr{H}^{\mathfrak{H}})$. Тогда $\mathscr{H}$ является $\Gamma_{\mathbb{G}}$-базисом идеала $(\mathscr{H})$ в том и только в том случае, если

$$\forall g = (g_h)_{h^{\mathfrak{H}} \in \mathscr{H}^{\mathfrak{H}}} \in \mathscr{B} \quad \mathbf{grem}\left(\sum_{h \in \mathscr{H}} g_h h, \mathscr{H}\right) = 0.$$

Алгоритм 3.1 (Построение $\Gamma_{\mathbb{G}}$-базиса)

```
# GammaBasisConstruction, ℋ_Δ — множество полиномов, порождающих идеал.
def GammaBasisConstruction(ℋ_Δ):
.    ℋ = ℋ_Δ
.    flag = true
.    while(flag):
.    .    flag = false
.    .    ℬ = BasisSyz(ℋ^𝔥 ) # Вычисляет базис S(ℋ^𝔥).
.    .    for g in ℬ:
.    .    .    r = grem(∑ g_h h, ℋ)
.    .    .    if(r != 0):
.    .    .    .    ℋ = ℋ ∪ {r}
.    .    .    .    flag = true
.    .    .    .    break
.    return ℋ
# end-of-GammaBasisConstruction
```

Замечание 3.1 Представленный выше алгоритм полностью основан на следствии 3.2 и лемме Цорна и, безусловно, не является эффективным (хотя бы потому, что на каждом шагу приходится заново вычислять редуцированный базис Грёбнера для того, чтобы найти базис $S(\mathscr{H}^{\mathfrak{H}})$, что уже накладывает многие ограничения). Тем не менее, используя уже имеющиеся результаты из теории базисов Грёбнера, можно несколько улучшить и этот алгоритм (прежде всего такого рода модификации направлены на использование имеющегося базиса модуля сизигий на следующем шаге для вычисления нового).

Примеры:

3.1) Вернёмся к уже рассмотренному нами в разделе 1 идеалу $I = (h_1, h_2) \lhd \mathbb{R}[x, y]$, где

$$h_1 = x^3y - xy^3, \quad h_2 = x^4 + 2x^2y^2 + y^4 - 1.$$

Покажем с помощью алгоритма 3.1, что $\mathscr{H} = \{h_1, h_2\}$ является $\Gamma_{\mathbf{H}}$-базисом. Действительно, достаточно лишь один раз воспользоваться критерием из следствия 3.2. В нашем случае $S(\mathscr{H}^{\mathfrak{H}})$ порождается $(x^4 + 2x^2y^2 + y^4, -x^3y + xy^3)$. Имеем:

$$(x^4 + 2x^2y^2 + y^4)h_1 + (-x^3y + xy^3)h_2 = (h_2 + 1)h_1 - h_1h_2 = h_1 \rightarrowtail 0 \pmod{\mathscr{H}, \Gamma_{\mathbf{H}}}.$$

Мы вновь используем здесь обозначение из раздела 1, но при этом уже имея в виду конкретный алгоритм редукции, в данном случае алгоритм $\Gamma_{\mathbf{H}}$-редукции. Критерий выполнен, и следовательно, $\mathscr{H}$ является $\Gamma_{\mathbf{H}}$-базисом идеала I.

4. Вопросы из теории базисов Грёбнера

Обсуждая $\Gamma_{\mathbb{G}}$-базисы и исследуя их свойства, можно задаться вопросами, которые возникали при изучении базисов Грёбнера. В этом разделе мы на примерах постараемся показать, чем принципиально отличаются эти объекты, а в следующем разделе поговорим о приложениях $\Gamma_{\mathbb{G}}$-базисов к задачам полиномиальной интерполяции, где они существенно расширят наши возможности по сравнению с теми, что давали стандартные базисы.

Как было уже отмечено выше, алгоритм 3.1 (несмотря на все имеющиеся на сегодняшний день улучшения, в т.ч. и для регулярных последовательностей полиномов с использованием алгоритма F5, см. [6]) не позволяет эффективно вычислять $\Gamma_{\mathbb{G}}$-базисы. Но, тем не менее, одна из поставленных целей достигнута. Благодаря описанной в предыдущих разделах конструкции формально мы избавились от зависимости от порядка на мономах и можем использовать те градуировки на пространстве полиномов, которые нас интересуют, например, можно мыслить каждый полином как набор однородных компонент, т.е. использовать градуировку $\mathbf{H}$. Уже здесь стоит отметить, что мы не зря уделяли особое внимание именно этой градуировке. Именно она позволяет интерпретировать уже имеющиеся результаты в теории полиномиальной интерполяции в терминах коммутативной алгебры. В связи с этим возникают некоторые приятные «побочные эффекты» и отличия от стандартного базиса. Проиллюстрируем это на примерах. Сразу подчеркнём существенное отличие от теории Грёбнера: использование $\Gamma_{\mathbb{G}}$-базиса невозможно, если заранее не выбрать какое-нибудь скалярное произведение на пространстве $\mathfrak{P}$. При этом здесь и далее мы для простоты считаем, что $\mathbb{K} = \mathbb{R}$, это упростит выкладки. Можно взять самое простое скалярное произведение, которое использовал ещё Маколей в [7], именно, для $p = \sum p_\gamma x^\gamma$ и $q = \sum q_\gamma x^\gamma$ положим

$$(p, q)_M \stackrel{\text{def}}{=} \sum_{\gamma \in \mathbb{Z}^n_{\geqslant 0}} p_\gamma q_\gamma.$$

Примеры:
4.1) Рассмотрим идеал $I = (h_1, h_2) \lhd \mathbb{R}[x, y]$, $h_1 = 3x^2 + y^2 - 1$, $h_2 = x^2 + 3y^2 - 1$. Как и в примере 3.1, легко проверяется, что порождающие I полиномы уже образуют $\Gamma_{\mathbf{H}}$-базис. Используя скалярное произведение $(\cdot, \cdot)_M$, мы видим, что они не редуцированы относительно друг друга. Это наводит на мысль рассмотреть *редуцированный* $\Gamma_{\mathbf{H}}$-базис, в данном примере его легко получить непосредственно:

$$\widetilde{h}_1 = \frac{h_1 + h_2}{2} = 2x^2 + 2y^2 - 1, \;\; \widetilde{h}_2 = \frac{h_1 - h_2}{2} = x^2 - y^2.$$

Здесь сразу бросается в глаза симметрия полиномов $\widetilde{h}_1$ и $\widetilde{h}_2$, это и есть один из «побочных эффектов» нашей конструкции.

Несмотря на внешнюю простоту скалярного произведения $(\cdot, \cdot)_M$ для нас больший интерес (особенно это касается следующего раздела) будет представлять так называемое *каноническое* скалярное произведение. Для каждого монома x^γ пусть

$$\gamma! \stackrel{\text{def}}{=} \prod_{i=1}^{n} \gamma_i!.$$

Осуществим нормировку коэффициентов полиномов p и q, т.е. пусть

$$p = \sum_{\gamma \in \mathbb{Z}^n_{\geqslant 0}} p_\gamma \frac{x^\gamma}{\gamma!}, \quad q = \sum_{\gamma \in \mathbb{Z}^n_{\geqslant 0}} q_\gamma \frac{x^\gamma}{\gamma!}.$$

Определение 4.1 *Каноническим скалярным произведением* (на $\mathfrak{P}$) полиномов p и q называется скалярное произведение

$$(p,q)_{\mathfrak{C}} \stackrel{\text{def}}{=} \sum_{\gamma \in \mathbb{Z}^n_{\geqslant 0}} \frac{p_\gamma q_\gamma}{\gamma!}.$$

Примеры:
4.2) Множество $\{\widetilde{h}_1, \widetilde{h}_2\}$ из примера 4.1 является редуцированным $\Gamma_{\mathbf{H}}$-базисом и по отношению к каноническому скалярному произведению $(\cdot,\cdot)_{\mathfrak{C}}$.

Пусть теперь

$$p(D) \stackrel{\text{def}}{=} p\left(\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\right).$$

Утверждение 4.1 $(p,q)_{\mathfrak{C}} = (p(D)q)(0)$ для любых полиномов $p, q \in \mathfrak{P}$.

Следствие 4.1 $(pq, r)_{\mathfrak{C}} = (p, q(D)r)_{\mathfrak{C}}$ для любых $p, q, r \in \mathfrak{P}$.

Следствие 4.2 Если полином f редуцирован по отношению к $\Gamma_{\mathbf{H}}$-базису $\mathscr{H}$ и $(\cdot,\cdot)_{\mathfrak{C}}$, то и все производные f редуцированы.

Из следствия 4.2 немедленно вытекает, что пространство $\mathbf{grem}(\mathfrak{P}, \mathscr{H})$ замкнуто относительно операции дифференцирования. Наличие этого важного свойства (которое ещё называют *D-инвариантностью*, подробнее см. [9]) показывает, чем принципиально отличаются скалярные произведения $(\cdot,\cdot)_{\mathfrak{C}}$ и $(\cdot,\cdot)_M$, т.к. для последнего оно не выполнено. Проиллюстрируем это на следующем примере.

Примеры:
4.3) Рассмотрим множество $\mathscr{H} = \{x + y, x^3 - x^2y + xy^2 - y^3\}$, которое является редуцированным $\Gamma_{\mathbf{H}}$-базисом идеала $(\mathscr{H}) \lhd \mathbb{R}[x,y]$. Нетрудно убедиться, что относительно $(\cdot,\cdot)_M$

$$\mathbf{grem}(\mathfrak{P}, \mathscr{H}) = \langle x^2 - xy + y^2, x - y, 1\rangle.$$

Тем не менее, полином

$$\frac{\partial}{\partial x}(x^2 - xy + y^2) = 2x - y \notin \mathbf{grem}(\mathfrak{P}, \mathscr{H}).$$

Следовательно, пространство редуцированных полиномов не является D-инвариантным.

Вновь проводя сравнение $\Gamma_{\mathbb{G}}$-базисов и базисов Грёбнера, можно спросить: единственен ли редуцированный $\Gamma_{\mathbb{G}}$-базис для данного идеала I и фиксированного скалярного произведения? Увы, если для базисов Грёбнера это так, то даже для $\Gamma_{\mathbf{H}}$-базисов ничего подобного не происходит, как показывает следующий пример.

Примеры:
4.4) Рассмотрим идеал $I = (h_1, h_2) \lhd \mathbb{R}[x, y]$, полагая $h_1 = x^4 + y^4 - 1, h_2 = x^3y - xy^3$. Как и раньше, непосредственно проверяем, что полиномы h_1, h_2 уже образуют редуцированный $\Gamma_{\mathbf{H}}$-базис относительно $(\cdot, \cdot)_M$. Но у I существует и много других (и даже нормированных) редуцированных $\Gamma_{\mathbf{H}}$-базисов, например, таковым является любой из базисов $\{f_1, f_2\}$, где

$$f_1 = \lambda h_1 + \mu h_2, \;\; f_2 = -\mu h_1 + \lambda h_2, \;\; \lambda^2 + \mu^2 = 1.$$

За этим примером стоят весьма интересные факты из коммутативной алгебры, которые впервые доказал Маколей, а современное их изложение можно найти, например, в [2], п.6. В частности, если все элементы $\Gamma_{\mathbf{H}}$-базиса имеют одинаковую степень и непересекающиеся множества мономов однородных частей, то для него почти всегда можно построить такие семейства редуцированных $\Gamma_{\mathbf{H}}$-базисов, как приведённое выше.

Возвращаясь к теории базисов Грёбнера, стоит вспомнить ещё одну важную деталь. Когда нужно придумать какой-нибудь модельный пример базиса Грёбнера, не всегда обращаются, скажем, к алгоритму Бухбергера, а используют более простые достаточные условия для построения базиса. Одно такое условие, применяемое в случае $\Gamma_{\mathbf{H}}$-базисов, было использовано нами неоднократно. Впервые оно появилось в работах Маколея, его основой является доказанная им *теорема о несмешиваемости*. Впоследствии этот результат был обобщён, и мы приводим здесь его простую, но в то же время наиболее удобную на практике форму.

Теорема 4.1 (Слабая теорема о несмешиваемости) Пусть $\mathscr{H} = \{h_1, \ldots, h_n\} \subseteq \mathfrak{P}$. Если аффинное многообразие $\mathbf{V}(\mathscr{H}^{\mathfrak{H}}) = \{(0, \ldots, 0)\}$, то $\mathscr{H}$ — $\Gamma_{\mathbf{H}}$-базис идеала $(\mathscr{H})$.

Доказательство: [2], раздел 5.

Отметим, что эта теорема лежит в основе почти всех примеров, использованных в данной статье. Увы, более общая теорема сразу не даёт подобных результатов применительно к $\Gamma_{\mathbb{G}}$-базисам, но может быть использована для улучшения работы алгоритма 3.1 (в первую очередь это касается тех случаев, когда входная последовательность полиномов регулярна) путём добавления ряда критериев, которые действуют по схожему с критерями Бухбергера принципу.

5. Приложения к полиномиальной интерполяции

Одним из основных мест в вычислительной математике, где используются $\Gamma_{\mathbb{G}}$-базисы, являются вопросы, связанные с полиномиальной интерполяцией. Мы постараемся не углубляться в теорию, но, тем не менее, дадим все необходимые определения и докажем несколько теорем, которые позволят увидеть $\Gamma_{\mathbb{G}}$-базисы «в действии». Подробное обсуждение объектов полиномиальной интерполяции и их свойств можно найти в [8]. Все операции в данном разделе осуществляются над полем $\mathbb{R}$ относительно канонического скалярного произведения, введённого в предыдущем разделе. Для того чтобы осуществлять аналогичные действия над $\mathbb{C}$, достаточно лишь немного изменить каноническое скалярное произведение, именно, для $p, q \in \mathfrak{P}$ положить $(p, q) = (\overline{p}(D)q)(0)$.

Определение 5.1 Конечное множество линейно независимых функций $\Theta \subseteq \mathfrak{P}^*$ называется *интерполяционной схемой идеала* I кольца $\mathfrak{P}$, если

$$I = \ker \Theta \overset{\text{def}}{=} \{f \,|\, \forall \theta \in \Theta \;\; \theta(f) = 0\}.$$

Конечномерное подпространство $\mathfrak{I} \subseteq \mathfrak{P}$ называется *интерполяционным пространством* по отношению к Θ, если

$$\forall f \in \mathfrak{P} \ \exists!\, g \in \mathfrak{I} \ \forall \theta \in \Theta \ \ \theta(f) = \theta(g).$$

Интерполяционным оператором для Θ и $\mathfrak{I}$ называется отображение $\mathfrak{A} : \mathfrak{P} \to \mathfrak{I}$, сопоставляющее полиному f указанный выше полином g.

Определение 5.2 Интерполяционное пространство $\mathfrak{I}$ называется *интерполяционным пространством минимальной* $\Gamma_{\mathbb{G}}$*-степени*, если

$$\forall f \in \mathfrak{P} \ \ \mathbf{d}_{\mathbb{G}}(\mathfrak{A}f) \leqslant \mathbf{d}_{\mathbb{G}}(f),$$

где $\mathfrak{A}$ — интерполяционный оператор для Θ и $\mathfrak{I}$.

Для данной интерполяционной схемы Θ, вообще говоря, может существовать много интерполяционных пространств минимальной $\Gamma_{\mathbb{G}}$-степени, и выбор наиболее подходящего для решения тех или иных проблем является нетривиальной задачей. Один из возможных подходов к ней даёт следующая теорема, в которой главную роль играют именно $\Gamma_{\mathbb{G}}$-базисы.

Теорема 5.1 Пусть Θ – интерполяционная схема идеала I, $\mathscr{H}$ — его $\Gamma_{\mathbb{G}}$-базис. Тогда $\mathfrak{I}_{\mathscr{H}} = \mathbf{grem}(\mathfrak{P}, \mathscr{H})$ является интерполяционным пространством минимальной $\Gamma_{\mathbb{G}}$-степени, интерполяционный оператор $\mathfrak{A}$ которого имеет вид:

$$\mathfrak{A}f = \mathbf{grem}(f, \mathscr{H}).$$

Доказательство: Для любого $f \in \mathfrak{P}$

$$f - \mathbf{grem}(f, \mathscr{H}) \in I = \ker \Theta,$$

откуда следует, что для любого $\theta \in \Theta$

$$\theta(\mathbf{grem}(f, \mathscr{H})) = \theta(f - (f - \mathbf{grem}(f, \mathscr{H}))) = \theta(f) - \theta(f - \mathbf{grem}(f, \mathscr{H})) = \theta(f).$$

Тогда $\mathfrak{I}_{\mathscr{H}}$ является интерполяционным пространством по отношению к Θ. При этом

$$\mathbf{d}_{\mathbb{G}}(\mathfrak{A}f) = \mathbf{d}_{\mathbb{G}}(\mathbf{grem}(f, \mathscr{H})) \leqslant \mathbf{d}_{\mathbb{G}}(f),$$

откуда следует, что $\mathfrak{I}_{\mathscr{H}}$ — интерполяционное пространство минимальной $\Gamma_{\mathbb{G}}$-степени. □

Замечание 5.1 Теорема 5.1 иллюстрирует один из тех случаев, когда нам в сущности интересны не столько свойства самого Θ, сколько идеала $\ker \Theta$ и его $\Gamma_{\mathbb{G}}$-базиса. Это соответствие позволяет интерпретировать многие вопросы интерполяции минимальной степени в терминах теории Маколея (подробнее см. [7]).

Определение 5.3 Градуировка $\mathbb{M} = \{\mathscr{P}_\gamma \,|\, \gamma \in \Gamma\}$, индуцируемая Γ на $\mathfrak{P}$, называется *мономиальной*, если у каждого из пространств $\mathscr{P}_\gamma$ существует базис, состоящий только из мономов.

Примеры:
5.1) Градуировки $\mathbf{H}$ и $\mathbf{G}$, как легко видеть, являются мономиальными.

Теперь можно сформулировать некоторое обобщение утверждения 4.1, которое проверяется

непосредственно. Именно оно объясняет, почему в такого рода приложениях используется скалярное произведение $(\cdot,\cdot)_{\mathfrak{C}}$, а не $(\cdot,\cdot)_M$.

Утверждение 5.1 Для любой мономиальной градуировки $(\mathscr{P}_\gamma, \mathscr{P}_{\widetilde{\gamma}})_{\mathfrak{C}} = 0$ при $\gamma \neq \widetilde{\gamma}$.

Определение 5.4 Пусть Θ — интерполяционная схема идеала I. *Наименьшим интерполяционным* $\Gamma_{\mathbb{G}}$*-пространством* для Θ называется пространство

$$\mathfrak{I}^L_{\mathbb{G}}(\Theta) \stackrel{\text{def}}{=} \bigcap_{f\in I} \ker f^{\mathfrak{H}}(D).$$

Теорема 5.2 Пусть Θ — интерполяционная схема идеала I, $\mathscr{H}$ — его $\Gamma_{\mathbb{M}}$-базис относительно мономиальной градуировки $\mathbb{M}$. Тогда полином $q \in \mathfrak{P}$ является редуцированным относительно $\mathscr{H}$ и $(\cdot,\cdot)_{\mathfrak{C}}$, если и только если

$$q \in \bigcap_{h\in\mathscr{H}} \ker h^{\mathfrak{H}}(D) = \mathfrak{I}^L_{\mathbb{M}}(\Theta).$$

Доказательство: Предположим, что q является $\Gamma_{\mathbb{M}}$-компонентой, т.е.

$$q = \sum_{\mathbf{d}_{\mathbb{M}}(x^\beta)=\mathbf{d}_{\mathbb{M}}(q)} q_\beta \frac{x^\beta}{\beta!}.$$

Пусть теперь $p \in \mathfrak{P}$. Если $\mathbf{d}_{\mathbb{M}}(q) < \mathbf{d}_{\mathbb{M}}(p)$, то $p^{\mathfrak{H}}(D)q = 0$. Если же $\mathbf{d}_{\mathbb{M}}(q) \geqslant \mathbf{d}_{\mathbb{M}}(p)$, то

$$p^{\mathfrak{H}}(D)q = \sum_{\mathbf{d}_{\mathbb{M}}(x^\alpha)=\mathbf{d}_{\mathbb{M}}(p)} \frac{p_\alpha}{\alpha!}\frac{\partial^{|\alpha|}}{\partial x^\alpha}\left(\sum_{\mathbf{d}_{\mathbb{M}}(x^\beta)=\mathbf{d}_{\mathbb{M}}(q)} q_\beta \frac{x^\beta}{\beta!}\right) =$$

$$= \sum_{\mathbf{d}_{\mathbb{M}}(x^\alpha)=\mathbf{d}_{\mathbb{M}}(p)} \left(\sum_{\mathbf{d}_{\mathbb{M}}(x^\beta)=\mathbf{d}_{\mathbb{M}}(q)} \frac{p_\alpha q_\beta}{\alpha!(\beta-\alpha)!} x^{\beta-\alpha}\right) =$$

$$= \sum_{\mathbf{d}_{\mathbb{M}}(x^\gamma)=\mathbf{d}_{\mathbb{M}}(q)-\mathbf{d}_{\mathbb{M}}(p)} \left(\sum_{\mathbf{d}_{\mathbb{M}}(x^\beta)=\mathbf{d}_{\mathbb{M}}(p)} \frac{p_{\beta-\gamma} q_\beta}{(\beta-\gamma)!\gamma!}\right) x^\gamma = \sum_{\mathbf{d}_{\mathbb{M}}(x^\gamma)=\mathbf{d}_{\mathbb{M}}(q)-\mathbf{d}_{\mathbb{M}}(p)} (x^\gamma p^{\mathfrak{H}}, q)_{\mathfrak{C}} \cdot x^\gamma.$$

Тогда $p^{\mathfrak{H}}(D)q = 0$, если и только если

$$\forall f \in \mathfrak{X}\ \ (f,q)_{\mathfrak{C}} = 0, \text{ где } \mathfrak{X} = \{x^\gamma p^{\mathfrak{H}} \mid \mathbf{d}_{\mathbb{M}}(x^\gamma) = \mathbf{d}_{\mathbb{M}}(q) - \mathbf{d}_{\mathbb{M}}(p)\}.$$

Т.к. множество полиномов $\{x^\gamma h^{\mathfrak{H}} \mid \mathbf{d}_{\mathbb{M}}(x^\gamma) = \mathbf{d}_{\mathbb{M}}(q) - \mathbf{d}_{\mathbb{M}}(h), h \in \mathscr{H}\}$ порождает $V_{\mathbf{d}_{\mathbb{M}}(q)}(\mathscr{H})$, в силу линейности скалярного произведения получим, что

$$q \in \bigcap_{h\in\mathscr{H}} \ker h^{\mathfrak{H}}(D) \Longleftrightarrow q \perp V_{\mathbf{d}_{\mathbb{M}}(q)}(\mathscr{H})$$

Т.к. q по предположению является $\Gamma_{\mathbb{M}}$-компонентой, последнее равносильно тому, что q редуцирован. В том случае, если q представляется в виде суммы нескольких $\Gamma_{\mathbb{M}}$-компонент, проводя аналогичные рассуждениях для каждой из них, мы получим, что

$$q \in \bigcap_{h\in\mathscr{H}} \ker h^{\mathfrak{H}}(D) \Longleftrightarrow q \in \mathbf{grem}(\mathfrak{P}, \mathscr{H}).$$

Осталось проверить, что

$$\mathfrak{I}^L_{\mathbb{M}}(\Theta) = \bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D).$$

Включение

$$\mathfrak{I}^L_{\mathbb{M}}(\Theta) \subseteq \bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D)$$

тривиально. Для доказательства обратного рассмотрим полиномы $p \in \mathfrak{P}$ и $q \in \ker h^{\mathfrak{H}}(D)$, $h \in \mathscr{H}$. Имеем:

$$(ph)^{\mathfrak{H}}(D)q = (p^{\mathfrak{H}}(D)h^{\mathfrak{H}}(D))q = p^{\mathfrak{H}}(D)(h^{\mathfrak{H}}(D)q) = p^{\mathfrak{H}}(D)(0) = 0,$$

откуда в силу линейности дифференциальных операторов следует, что

$$q \in \bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D) \Longrightarrow q \in \bigcap_{h \in I} \ker h^{\mathfrak{H}}(D) \stackrel{\text{def}}{=} \mathfrak{I}^L_{\mathbb{M}}(\Theta),$$

это завершает доказательство. □

Следствие 5.1 Пусть Θ — интерполяционная схема идеала I, $\mathscr{H}$ — его $\Gamma_{\mathbb{M}}$-базис относительно мономиальной градуировки $\mathbb{M}$. Тогда $\mathfrak{I}^L_{\mathbb{M}}(\Theta)$ является интерполяционным пространством минимальной $\Gamma_{\mathbb{M}}$-степени по отношению к Θ и $(\cdot,\cdot)_{\mathfrak{C}}$, интерполяционный оператор которого имеет тот же вид, что и в теореме 5.1.

Замечание 5.2 Теорема 5.2 позволяет при решении ряда проблем компьютерной алгебры выбирать между интерполяцией и вычислением $\Gamma_{\mathbb{G}}$-базиса. Например, если множество Θ задано, то нужный $\Gamma_{\mathbb{G}}$-базис можно вычислить, используя только алгоритм $\Gamma_{\mathbb{G}}$-редукции, т.е. пользуясь лишь методом Гаусса (подробнее см. [10]). И наоборот, если множество Θ задано какой-то полиномиальной системой, для определения наименьшего интерполяционного $\Gamma_{\mathbb{G}}$-пространства совсем не обязательно вычислять соответствующий $\Gamma_{\mathbb{G}}$-базис, достаточно использовать $\Gamma_{\mathbb{G}}$-редукцию.

В заключение докажем ещё одну теорему, которая даёт весьма интересный критерий для определения того, является ли данное множество полиномов $\Gamma_{\mathbb{G}}$-базисом.

Теорема 5.3 Пусть $I = (\mathscr{H})$ — нульмерный идеал кольца $\mathfrak{P}$, где $\mathscr{H}$ — конечное множество полиномов. Тогда $\mathscr{H}$ является $\Gamma_{\mathbb{M}}$-базисом I относительно мономиальной градуировки $\mathbb{M}$, если и только если

$$\dim(\mathfrak{P}/I) = \dim\left(\bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D)\right).$$

Доказательство: Необходимость сразу следует из теоремы 5.2. Действительно, т.к. I — нульмерный идеал (т.е. идеал конечной коразмерности), для него существует какая-то интерполяционная схема Θ. По теореме 5.2 получаем, что

$$\dim(\mathfrak{P}/I) = \dim(\mathbf{grem}(\mathfrak{P},\mathscr{H})) = \dim\left(\bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D)\right).$$

Для доказательства достаточности рассмотрим ортогональные дополнения $V_d(\mathscr{H})$ относительно $(\cdot,\cdot)_{\mathfrak{C}}$ до всего пространства $\mathscr{P}_d$, т.е. пусть

$$\widetilde{V}_d(\mathscr{H}) \stackrel{\text{def}}{=} V_d(\mathscr{H})^{\perp} \subseteq \mathscr{P}_d, \;\; d \in \Gamma.$$

Докажем, что
$$\forall d \in \Gamma \quad \widetilde{V}_d(\mathscr{H}) \subseteq \bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D).$$
В силу утверждения 5.1 для любого полинома $q \in \mathfrak{P}$ имеет место представление:
$$q = \sum_{\gamma \in \mathbb{Z}^n_{\geqslant 0}} (x^\gamma, q)_{\mathfrak{C}} \cdot \frac{x^\gamma}{\gamma!}.$$
Тогда, положив $q \in \widetilde{V}_d(\mathscr{H})$ и взяв произвольный $h \in \mathscr{H}$, получим, что
$$h^{\mathfrak{H}}(D)q = \sum_{\gamma \in \mathbb{Z}^n_{\geqslant 0}} (x^\gamma, h^{\mathfrak{H}}(D)q)_{\mathfrak{C}} \cdot \frac{x^\gamma}{\gamma!} = \sum_{\gamma \in \mathbb{Z}^n_{\geqslant 0}} (x^\gamma h^{\mathfrak{H}}, q)_{\mathfrak{C}} \cdot \frac{x^\gamma}{\gamma!} = 0,$$
откуда следует, что
$$q \in \bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D).$$
В частности, из этого следует, что
$$\dim \left(\bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D) \right) \geqslant \sum_{d \in \Gamma} \dim \widetilde{V}_d(\mathscr{H}).$$
Т.к. $\forall d \in \Gamma \dim V_d(\mathscr{H}) \leqslant \dim (\mathscr{P}_d \cap I)$ и $\mathfrak{P} = \mathfrak{P}/I + I$,
$$\forall d \in \Gamma \quad \dim \widetilde{V}_d(\mathscr{H}) \geqslant \dim (\mathscr{P}_d \cap \mathfrak{P}/I),$$
причём равенство для всех $d \in \Gamma$ имеет место тогда и только тогда, когда
$$\forall d \in \Gamma \quad V_d(\mathscr{H}) = \mathscr{P}_d \cap I^{\mathfrak{H}},$$
т.е. когда $\mathscr{H}$ является $\Gamma_{\mathbb{M}}$-базисом I. Следовательно, если $\mathscr{H}$ не является $\Gamma_{\mathbb{M}}$-базисом, то
$$\sum_{d \in \Gamma} \dim \widetilde{V}_d(\mathscr{H}) > \sum_{d \in \Gamma} \dim (\mathscr{P}_d \cap \mathfrak{P}/I) = \dim (\mathfrak{P}/I).$$
Совмещая полученные неравенства, мы имеем:
$$\dim \left(\bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D) \right) > \dim (\mathfrak{P}/I),$$
что и доказывает искомое утверждение. □

Отсюда легко получить оценку сверху на коразмерность идеала.

Следствие 5.2 Пусть $\mathscr{H}$ — конечное множество полиномов. В предположениях предыдущей теоремы имеет место следующее неравенство:
$$\dim \left(\bigcap_{h \in \mathscr{H}} \ker h^{\mathfrak{H}}(D) \right) \geqslant \dim (\mathfrak{P}/(\mathscr{H})).$$

Список литературы

[1] D. Cox, J. Little, D. O'Shea, *"Ideals, Varieties, and Algorithms"*, Springer Verlag, 2007.
[2] H. M. Möller, T. Sauer, *"H-bases for polynomial interpolation and system solving"*, Advances Comput. Math., 12 (2000).
[3] T. Sauer, *"Gröbner bases, H-bases and interpolation"*, Trans. Amer. Math. Soc., 353 (2001).
[4] H. M. Möller, *"On the construction of Gröbner bases using syzygies"*, J. Symbolic Comput., 6 (1988).
[5] L. Robbiano, *"On the Theory of Graded Structures"*, J. Symbolic Comput., 2 (1986).
[6] J.-Ch. Faugère, *"A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)"*, 2004.
[7] F. S. Macaulay, *"The algebraic theory of modular systems"*, Cambridge Tracts in Math. and Math. Physics, 19, Cambridge Univ. Press, 1916.
[8] C. de Boor, A. Ron, *"On multivariate polynomial interpolation"*, Constr. Approx. 6 (1990)
[9] C. de Boor, A. Ron, *"The least solution for the polynomial interpolation problem"*, Math. Z. 210 (1992)
[10] C. de Boor, A. Ron, *Gauss elimination by segments and multivariate polynomial interpolation*, Approximation and Computation: A Festschrift in Honor of Walter Gautschi (R. V. M. Zahar, ed.), Birkhäuser Verlag, 1994